UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/975,410	10/10/2001	Jukka Vialen	930.339-US-W1	1295

32294 7590 05/05/2005

SQUIRE, SANDERS & DEMPSEY L.L.P.
14TH FLOOR
8000 TOWERS CRESCENT
TYSONS CORNER, VA 22182

EXAMINER	
CHOU, ALBERT T	
ART UNIT	**PAPER NUMBER**
2662	

DATE MAILED: 05/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/975,410	VIALEN ET AL.	
	Examiner	Art Unit	
	Albert T. Chou	2662	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *the amendment filed on 2/16/2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,6 and 9-24* is/are rejected.

7)☒ Claim(s) *4,5,7 and 8* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 February 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☒ Other: *See Continuation Sheet*.

Continuation of Attachment(s) 6). Other: 3G TS 33.102 V.3.3.1 Release 1999 (8 pages).

DETAILED ACTION

Claim Objections

1. Claim 3 is objected to because of the following informalities:

- Claim 3 was submitted as *"(Original) A method as claimed in claim 1, wherein a separate input is provided for said information relating to the identity of the channel"* in applicant's AMENDMENTS TO THE CLAIMS (page 5), filed on February 16, 2005. Based on examiner's telephone interview with Mr. David E. Brown on April 29, 2005, the applicant agreed that in response to this Office Action claim 3 will be amended to "*A method as claimed in claim 1, wherein said information relating to the identity of the channel is combined with at least one other input value*." as claimed in the Preliminary Amendment, which applicant submitted on October 10, 2001. Therefore, this Office Action is based on the October 10, 2001 version of claim 3.
- Claim 9, "*the output **to** an integrity algorithm*" should be "*the output **of** an integrity algorithm*".

Appropriate correction is required.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the

applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-3, 6 and 9-24 are rejected under 35 U.S.C. 102(e) as being anticipated by 3GPP TS 33.102 V3.3.1 (2000-01) Release 1999 (published date January 14, 2000), hereinafter referred to as 3GPP.

Regarding claims 1 and 19, 3GPP teaches a method of communication between a first node and second node **[Fig. 14, sec. 6.4.5]**, a plurality of different channels being provided between said first and second node, said method comprising the steps of:

calculating an integrity output **[Fig. 16; sec. 6.5.2; MAC-I and XMAC-I]**, said integrity output being calculated from a plurality of input values **[Fig. 16; sec. 6.5.2; IK, COUNT, FRESH, MESSAGE and DIRECTION]**, some of said input values being the same for said different channels **[Fig. 16; sec. 6.5.2; DIRECTION]**, at least one of said input values being arranged to comprise information related to the identity of said channel **[Fig. 16; sec. 6.5.2; MESSAGE]**, each channel having a different identity **[It is inherent in 3GPP wireless radio communications and well known in the art that there is a channel ID associated with each channel]** and at least one said input values are identical for said different channels **[Fig. 16; sec. 6.5.2; DIRECTION]** , and

transmitting information relating to the integrity output from one of said nodes to the other **[Sec. 6.5.2; The MAC-I is appended to the message when sent over the radio access link]**.

Regarding claim 2, 3GPP teaches a separate input is provided for said information relating to the identity of the channel **[Fig. 16; sec. 6.5.2; signaling data (MESSAGE)]**.

Regarding claim 3, 3PGG teaches a separate input is provided for said information relating to the identity of the channel **[Fig. 16; sec. 6.5.2; signaling data (MESSAGE)]**.

Regarding claim 6, 3PGG teaches values input to an algorithm comprise one or more of the following values: an integrity key; a direction value, a fresh value, a message value and a count value **[Fig. 16; sec. 6.5.2; IK, COUNT, FRESH, MESSAGE and DIRECTION]**.

Regarding claim 9, 3PGG teaches the output of the integrity algorithm is sent from one node to another **[Fig. 14; sec. 6.4.6; fig. 16; sec. 6.5.2; The MAC-I is appended to the message, the data, when sent over the radio access link by the transmitter. The receiver computes XMAC-I on the message received in the same way as the sender computed MAC-I on the message sent]**.

Regarding claim 10, 3PGG teaches the communication between the first and second nodes is via a wireless connection **[Sec. 6.5.2; The MAC-I is appended to the message, the data, when sent over the radio access link, which is a wireless connection]**.

Regarding claims 11 and 12, 3PGG teaches one of the first and second nodes is mobile station, the user equipment **[Fig. 14; sec. 6.4.6; sec. 6.5.1; A message**

authentication function shall be applies on the signaling information elements transmitter between the MS (mobile station), the user equipment, and the SN].

Regarding claims 13 and 14, 3PGG teaches one of the first and second nodes is a node B (base transceiver station), which is part of RNC **[Fig. 14; sec. 6.4.6; sec. 6.5.1; A message authentication function shall be applies on the signaling information elements transmitter between the MS (mobile station), the user equipment, and the SN, which includes RNC and base station transceiver]**.

Regarding claims 15 and 16, it is inherent and well known in the art of wireless radio communications that communication channels comprise signaling radio bearer for controlling the radio signaling and the data radio bearers for user data.

Regarding claim 17. 3PGG teaches the input values are input to an algorithm for calculation said output **[Fig. 16; sec. 6, 5.1 & 6.5.2; IK, COUNT, FRESH, MESSAGE and DIRECTION are inputs to UMTS Integrity Algorithm for calculating MAC-I, the output]**.

Regarding claim 18, 3PGG teaches the same integrity key is used for the different channels **[Sec. 6.4.3; Cipher key and integrity key life time]**

Regarding claim 20, 3GPP teaches a method of communication between a first node and a second node **[Fig. 14, sec. 6.4.5]**, a plurality of different channels being provided between said first and second node, said method comprising the steps of:

calculating an integrity output using a plurality of values, one of said values being an integrity key **[Fig. 16; sec. 6.5.2; IK, COUNT, FRESH, MESSAGE and DIRECTION]**, each of said channels having a different integrity key **[Sec. 6.4.1; Mutual**

key setting is the procedure that allows the NS and the RNC to agree on the key IK used to computer message authentication codes using UIA]; and transmitting information relating to the output of said an integrity algorithms from one of said nodes to the other **[Sec. 6.5.2; The MAC-I is appended to the message when sent over the radio access link from MS to SRNC]**.

Regarding claim 21, 3GPP teaches a method of communication between a first node and a second node **[Fig. 14, sec. 6.4.5]**, a plurality of different channels being provided between said first and second node, said method comprising:

triggering an authentication procedure **[Sec. 6.4.6; RNC may detect that new security parameters are needed. This may be triggered by failure of integrity checks, or at handover the new RNC does not support an algorithm selected by the old RNC]**; and

calculating a desired number of integrity parameters by the authentication procedure **[Sec. 6.4.6 & fig. 15, step 3; CN sends a security mode command to RNC. This will restart the integrity check with new parameters]**.

Regarding claim 22, 3GPP teaches a node **[Fig. 14, sec. 6.4.5; MS]**, the node for use in a system comprising a node and a further node **[Fig. 14, sec. 6.4.5; SRNC]**, a plurality of different channels being provided between two nodes, the node comprising means for calculating an integrity output **[Fig. 16; sec. 6.5.2; MAC-I]**, the integrity output being calculated from a plurality of values **[Fig. 16; sec. 6.5.2; IK, COUNT, FRESH, MESSAGE and DIRECTION]**, some of the values being the same for the different channels **[Fig. 16; sec. 6.5.2; DIRECTION]**, at least one of the values being

arranged to comprise information relating to the identity of the channel **[Fig. 16; sec. 6.5.2; MESSAGE]**, each channel having a different identity**[It is inherent in 3GPP wireless radio communications and well known in the art that there is a channel ID associated with each channel]**; and means for transmitting information relating to the integrity output from the node to the further node **[Sec. 6.5.2; The MAC-I is appended to the message when sent over the radio access link from MS to SRNC]**.

Regarding claim 23, 3GPP teaches a node **[Fig. 14, sec. 6.4.5; MS]**, the node for use in a system comprising a node and a further node **[Fig. 14, sec. 6.4.5; SRNC]**, a plurality of different channels being provided between two nodes, the node comprising means for calculating an integrity output **[Fig. 16; sec. 6.5.2; MAC-I]**, the integrity output being calculated from a plurality of values **[Fig. 16; sec. 6.5.2; IK, COUNT, FRESH, MESSAGE and DIRECTION]**, some of the values being the same for the different channels **[Fig. 16; sec. 6.5.2; DIRECTION]**, at least one of the values being arranged to comprise information relating to the identity of the channel **[Fig. 16; sec. 6.5.2; MESSAGE]**, each channel having a different identity**[It is inherent in 3GPP wireless radio communications and well known in the art that there is a channel ID associated with each channel]**; and means for comparing information relating to the integrity output calculated by the node with a value calculated by the further node **[Sec. 6.5.2; The receiver, SRNC, computes XMAC-I on the message received and verifies the data integrity of the message by comparing it to the received MAC-I].**

Regarding claim 24, 3GPP teaches an algorithm **[Sec. 6.5.2 Integrity Algorithm]** for calculating an integrity output for use in a system comprising a node and a further node, a plurality of different channels being provided between said nodes, said algorithm comprising means for calculating an integrity output **[Fig. 16; sec. 6.5.2; MAC-I]**, said integrity output being calculated from a plurality of values **[Fig. 16; sec. 6.5.2; IK, COUNT, FRESH, MESSAGE and DIRECTION]**, some of said values being the same for said different channels **[Fig. 16; sec. 6.5.2; DIRECTION]**, at least one of said values being arranged to comprise information relating to the identity of said channel **[Fig. 16; sec. 6.5.2; MESSAGE]**, each channel having a different identity **[It is inherent in 3GPP wireless radio communications and well known in the art that there is a channel ID associated with each channel]**.

Allowable Subject Matter

4. Claims 4, 5, 7 and 8 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Response to Arguments

5. Applicant's arguments with respect to claims 1-24 have been considered but are moot in view of the new ground(s) of rejection.

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Albert T. Chou whose telephone number is 571-272-6045. The examiner can normally be reached on 8:30 - 17:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hassan Kizou can be reached on 571-272-3088. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ac

Albert T. Chou
April 29, 2005

HASSAN KIZOU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600